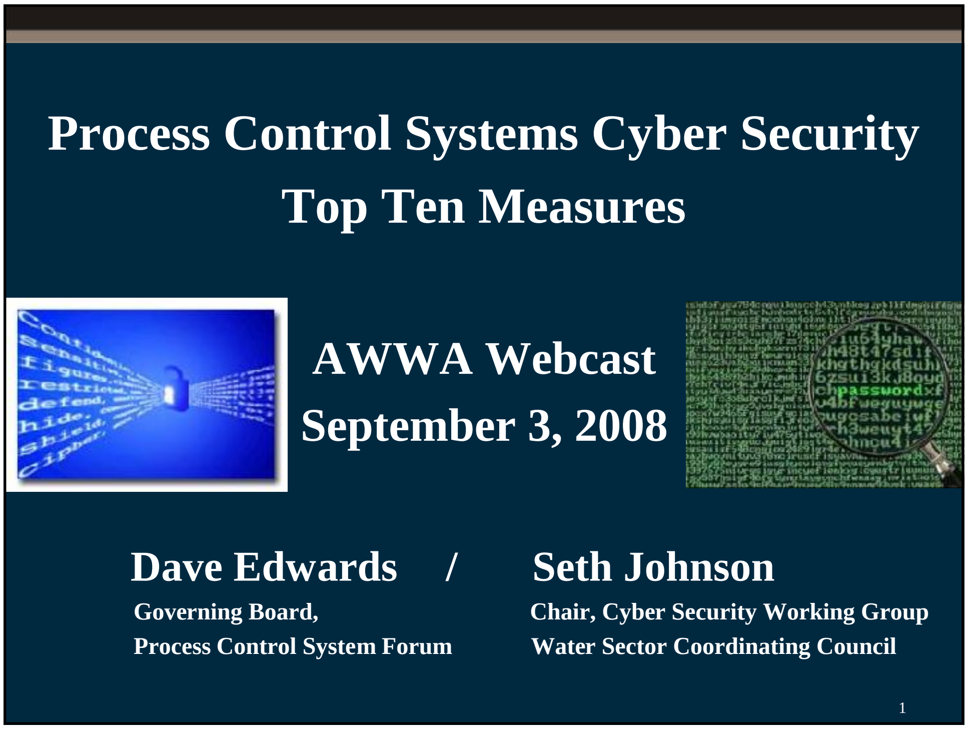


# Process Control Systems Cyber Security Top Ten Measures

AWWA Webcast
September 3, 2008

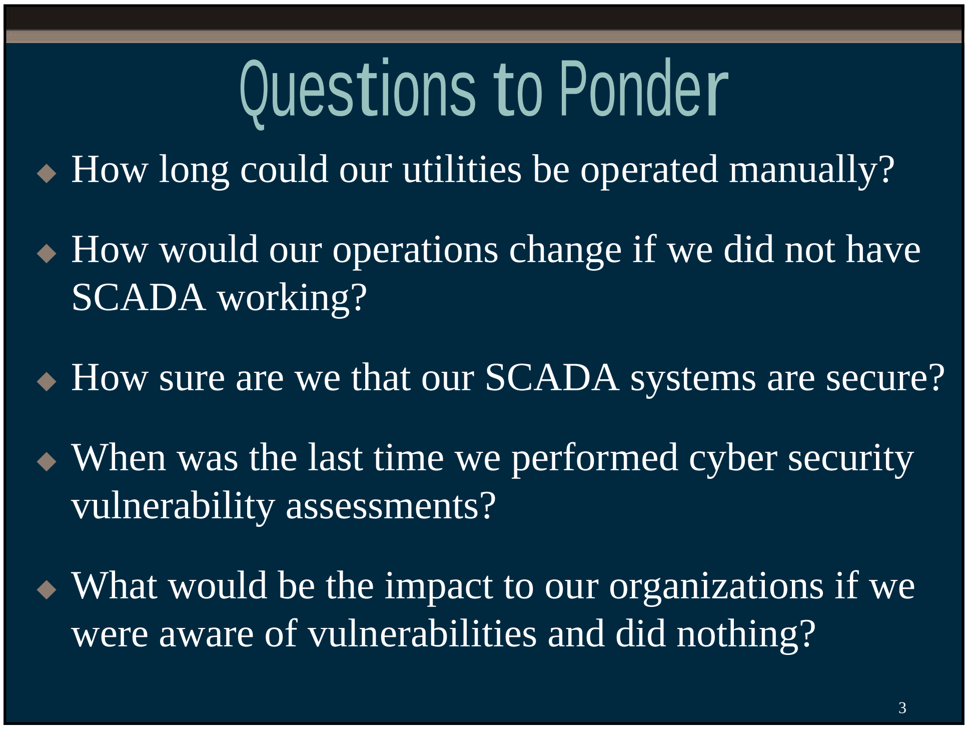
**Dave Edwards** / **Seth Johnson**

Governing Board,
Process Control System Forum

Chair, Cyber Security Working Group
Water Sector Coordinating Council

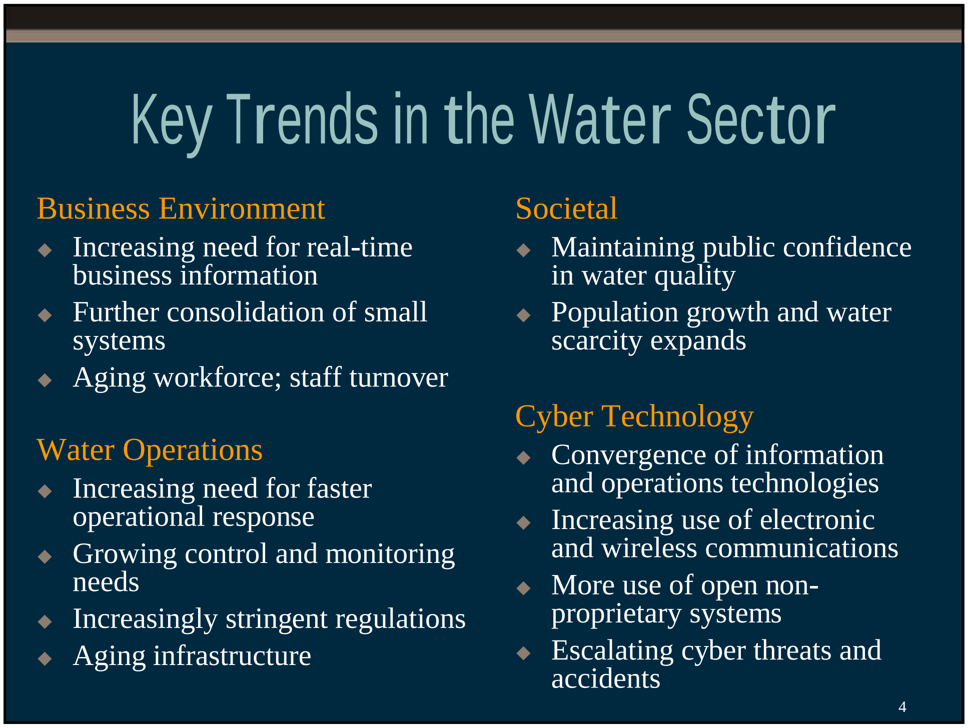
## Agenda

- Current Cyber Situation
- Challenges / Opportunities
- Top 10 Measures
- Water Sector Cyber Security Roadmap



## Questions to Ponder

- How long could our utilities be operated manually?
- How would our operations change if we did not have SCADA working?
- How sure are we that our SCADA systems are secure?
- When was the last time we performed cyber security vulnerability assessments?
- What would be the impact to our organizations if we were aware of vulnerabilities and did nothing?



## Key Trends in the Water Sector

### Business Environment

- Increasing need for real-time business information
- Further consolidation of small systems
- Aging workforce; staff turnover

### Water Operations

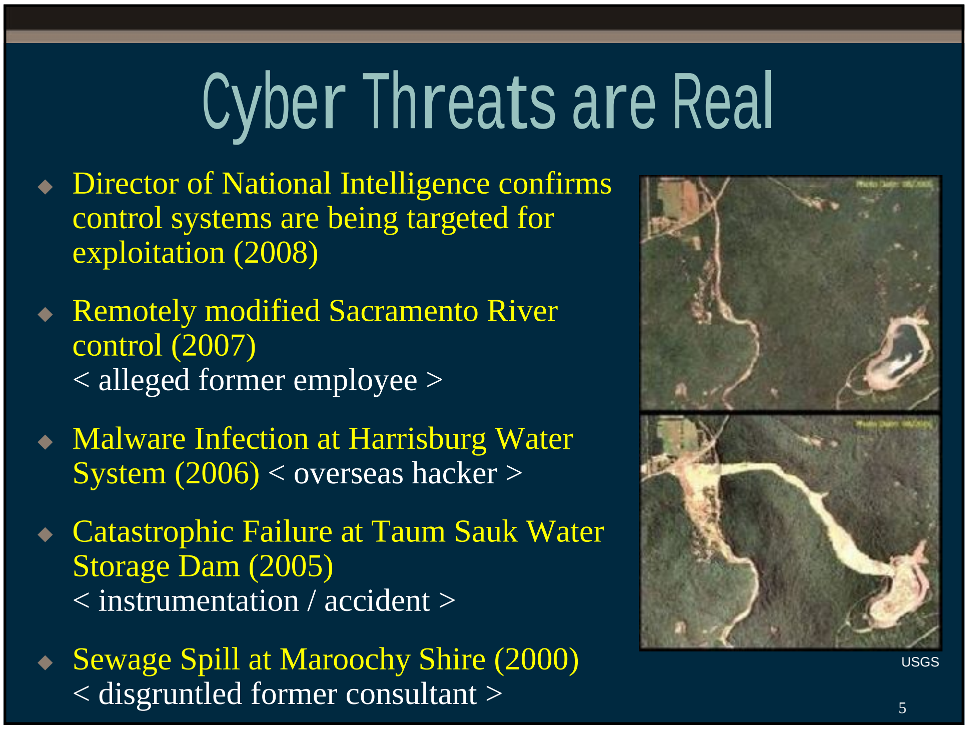
- Increasing need for faster operational response
- Growing control and monitoring needs
- Increasingly stringent regulations
- Aging infrastructure

### Societal

- Maintaining public confidence in water quality
- Population growth and water scarcity expands

### Cyber Technology

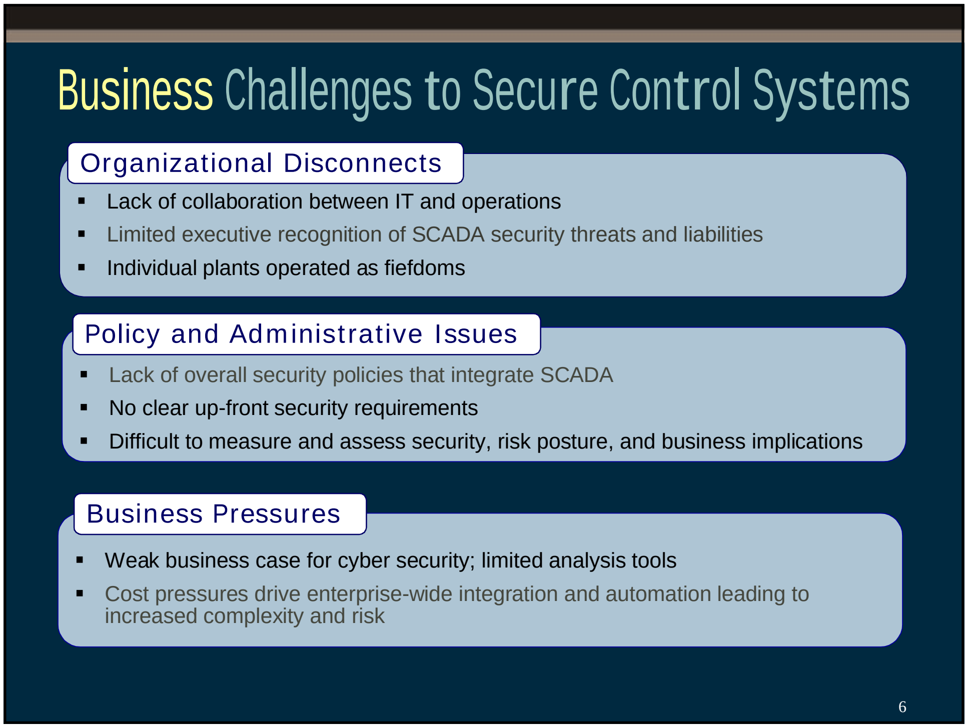
- Convergence of information and operations technologies
- Increasing use of electronic and wireless communications
- More use of open non-proprietary systems
- Escalating cyber threats and accidents



# Cyber Threats are Real

- Director of National Intelligence confirms control systems are being targeted for exploitation (2008)
- Remotely modified Sacramento River control (2007)
  < alleged former employee >
- Malware Infection at Harrisburg Water System (2006) < overseas hacker >
- Catastrophic Failure at Taum Sauk Water Storage Dam (2005)
  < instrumentation / accident >
- Sewage Spill at Maroochy Shire (2000)
  < disgruntled former consultant >

USGS



# Business Challenges to Secure Control Systems

## Organizational Disconnects

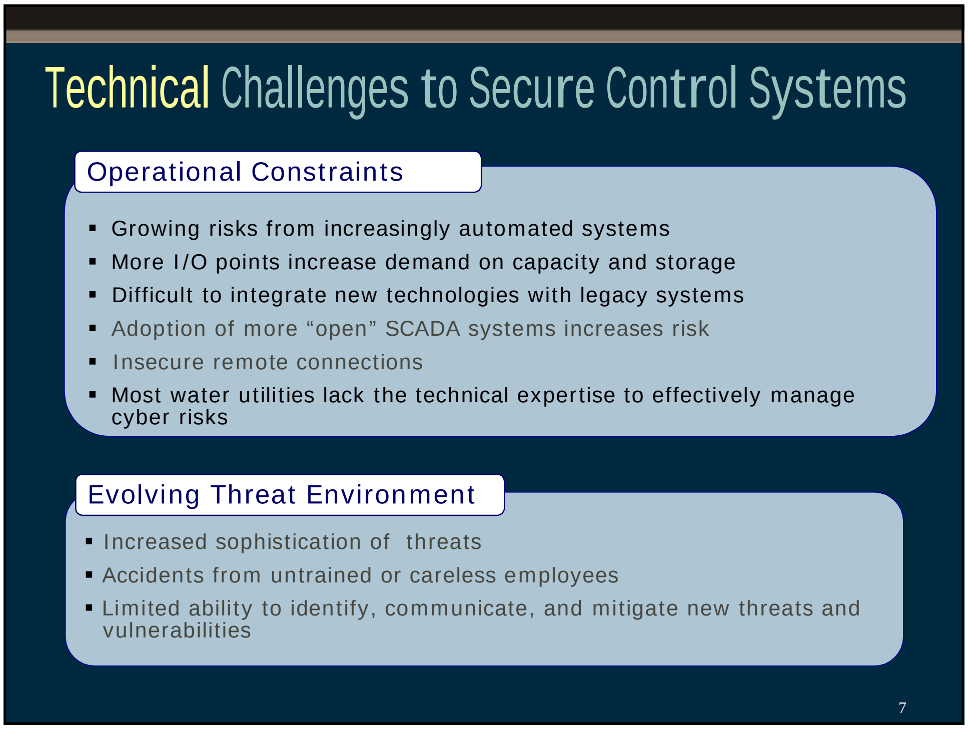
- Lack of collaboration between IT and operations
- Limited executive recognition of SCADA security threats and liabilities
- Individual plants operated as fiefdoms

## Policy and Administrative Issues

- Lack of overall security policies that integrate SCADA
- No clear up-front security requirements
- Difficult to measure and assess security, risk posture, and business implications

## Business Pressures

- Weak business case for cyber security; limited analysis tools
- Cost pressures drive enterprise-wide integration and automation leading to increased complexity and risk



## Technical Challenges to Secure Control Systems

### Operational Constraints

- Growing risks from increasingly automated systems
- More I/O points increase demand on capacity and storage
- Difficult to integrate new technologies with legacy systems
- Adoption of more “open” SCADA systems increases risk
- Insecure remote connections
- Most water utilities lack the technical expertise to effectively manage cyber risks

### Evolving Threat Environment

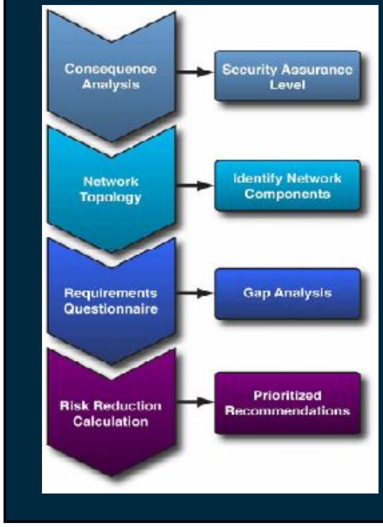
- Increased sophistication of threats
- Accidents from untrained or careless employees
- Limited ability to identify, communicate, and mitigate new threats and vulnerabilities

## Top 10 Measures

# What Should My Utility Have In Place?

1. Periodic vulnerability assessments
2. Limited/protected connections to the control system network
3. Network monitoring/protection
4. Hardened configuration for control system components
5. Strong authentication methods
6. Regular antivirus updates and patch management
7. Testing and backup practices for control system
8. Strong physical security for control system components
9. Background checks on individuals touching control system
10. Most knowledgeable resources working collaboratively

# Vulnerability Assessments

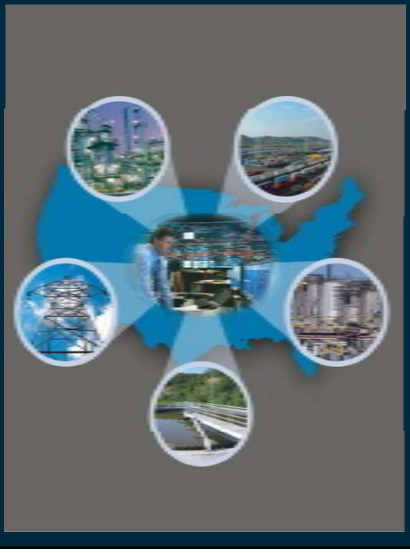


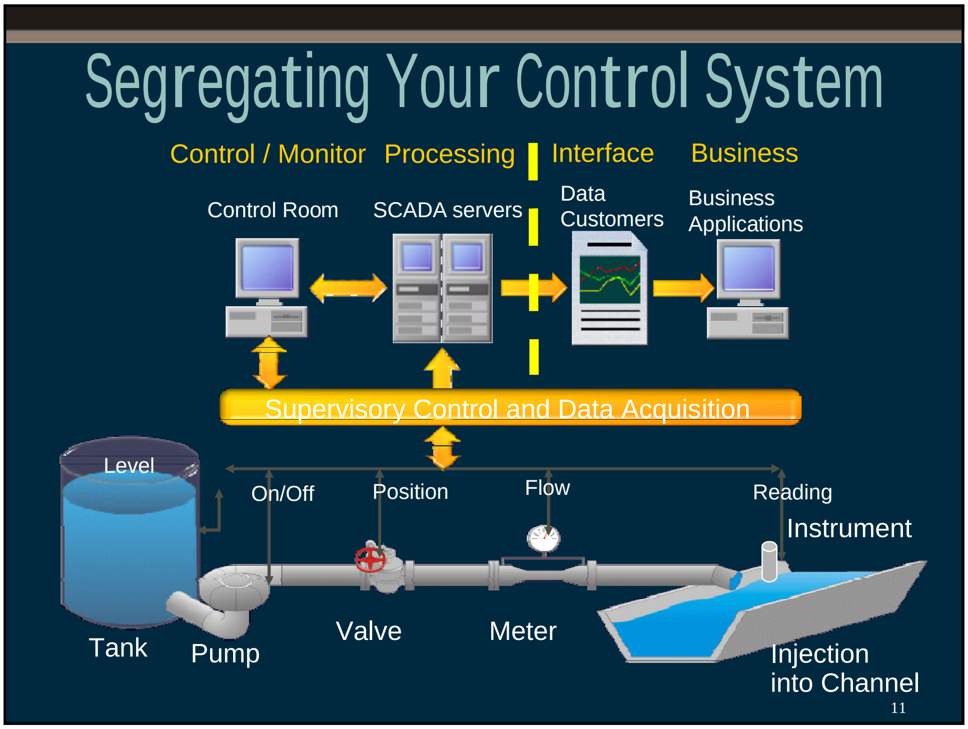
Consequence Analysis → Security Assurance Level

Network Topology → Identify Network Components

Requirements Questionnaire → Gap Analysis

Risk Reduction Calculation → Prioritized Recommendations





# Segregating Your Control System

Control / Monitor

Processing

Interface

Business

Control Room

SCADA servers

Data Customers

Business Applications

Supervisory Control and Data Acquisition

Level

On/Off

Position

Flow

Reading

Instrument

Tank

Pump

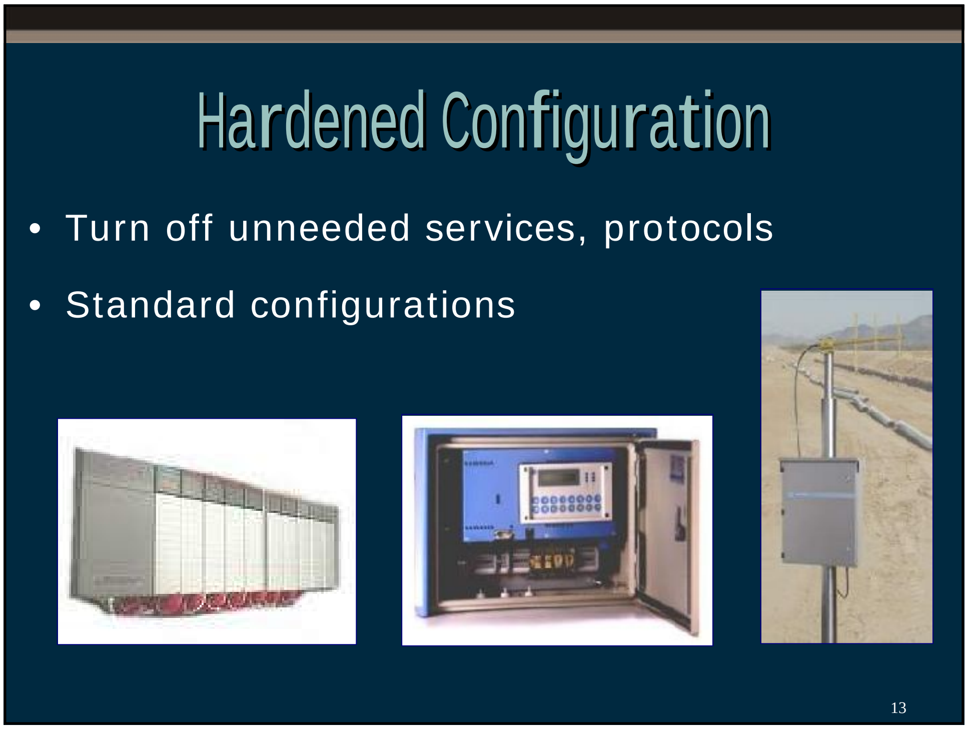
Valve

Meter

Injection into Channel

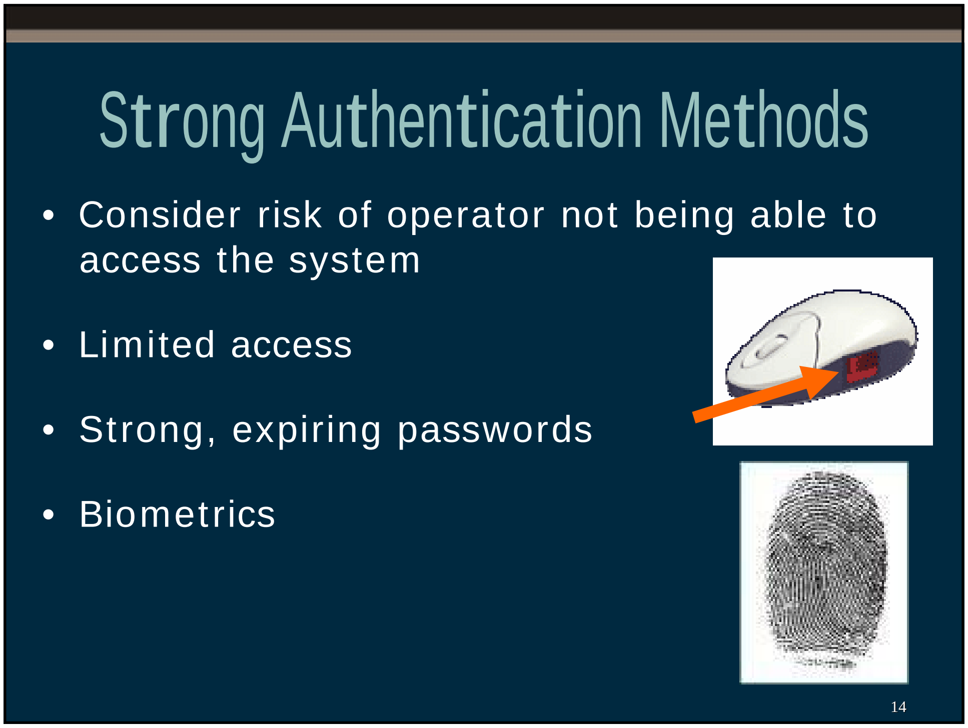
# Network Monitoring / Protection

- Intrusion Detection
- Intrusion Prevention?
- Auditing and Logging



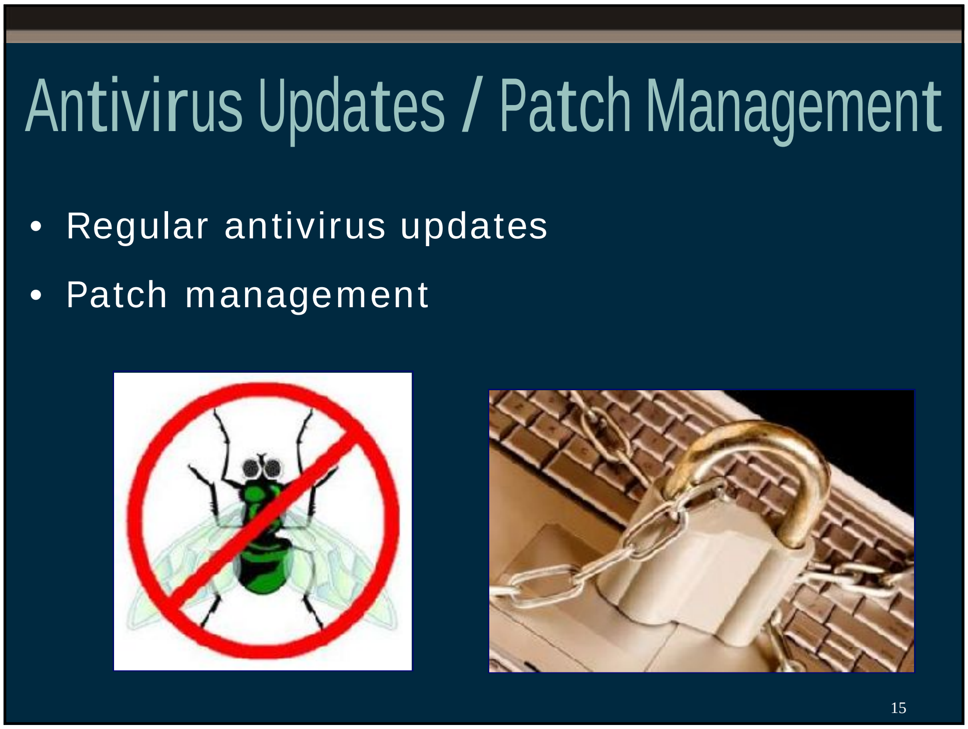
## Hardened Configuration

- Turn off unneeded services, protocols
- Standard configurations



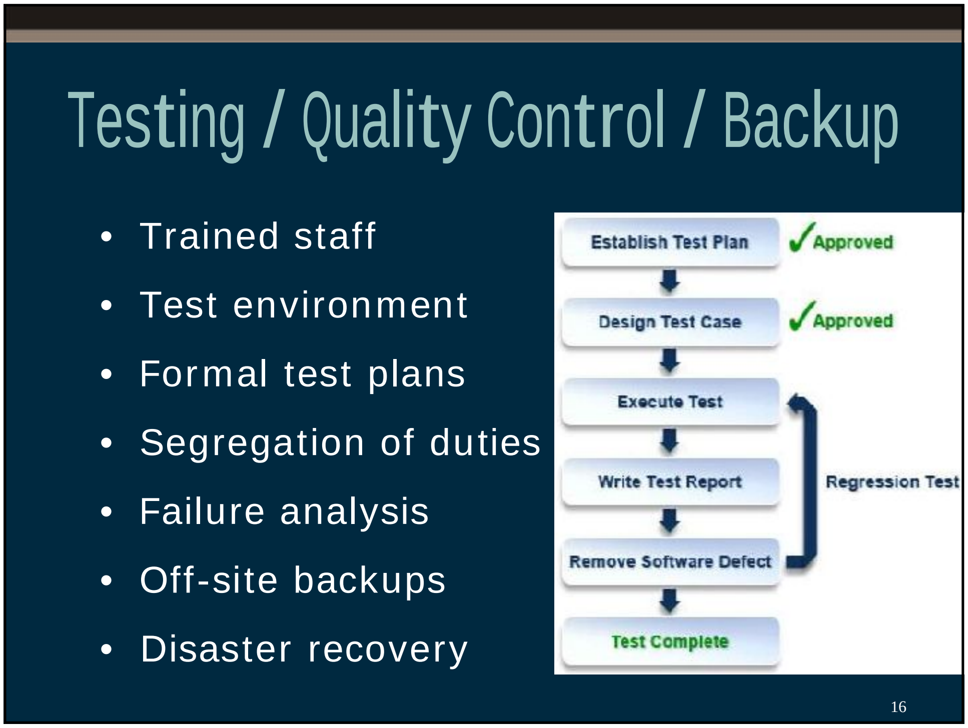
## Strong Authentication Methods

- Consider risk of operator not being able to access the system
- Limited access
- Strong, expiring passwords
- Biometrics



## Antivirus Updates / Patch Management

- Regular antivirus updates
- Patch management



## Testing / Quality Control / Backup

- Trained staff
- Test environment
- Formal test plans
- Segregation of duties
- Failure analysis
- Off-site backups
- Disaster recovery

Establish Test Plan ✓Approved

Design Test Case ✓Approved

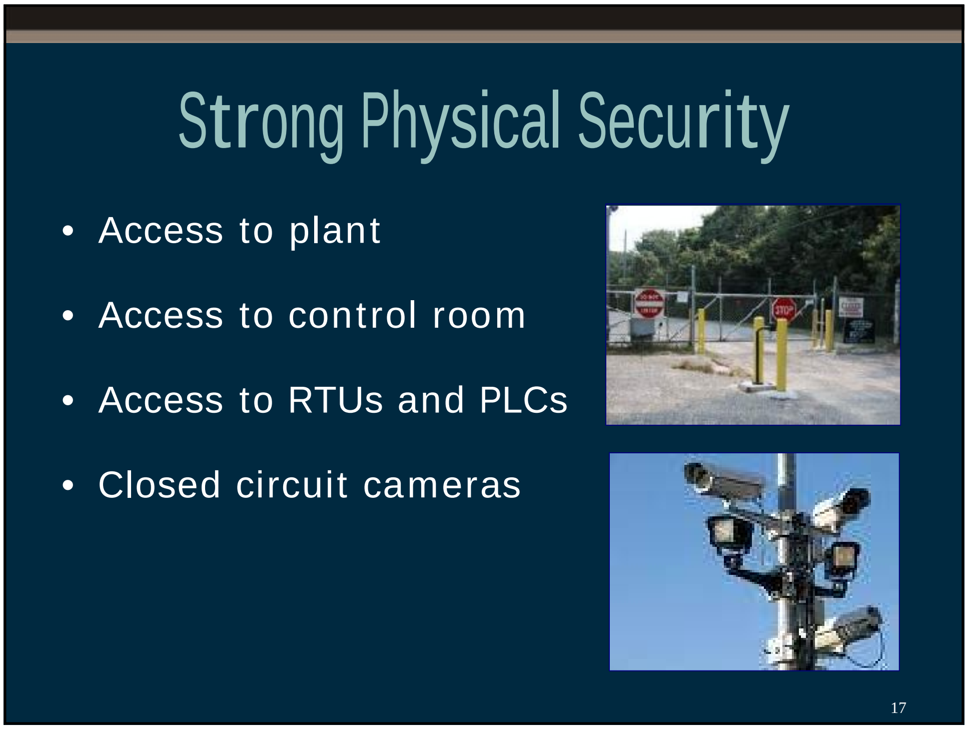
Execute Test

Write Test Report

Remove Software Defect

Regression Test

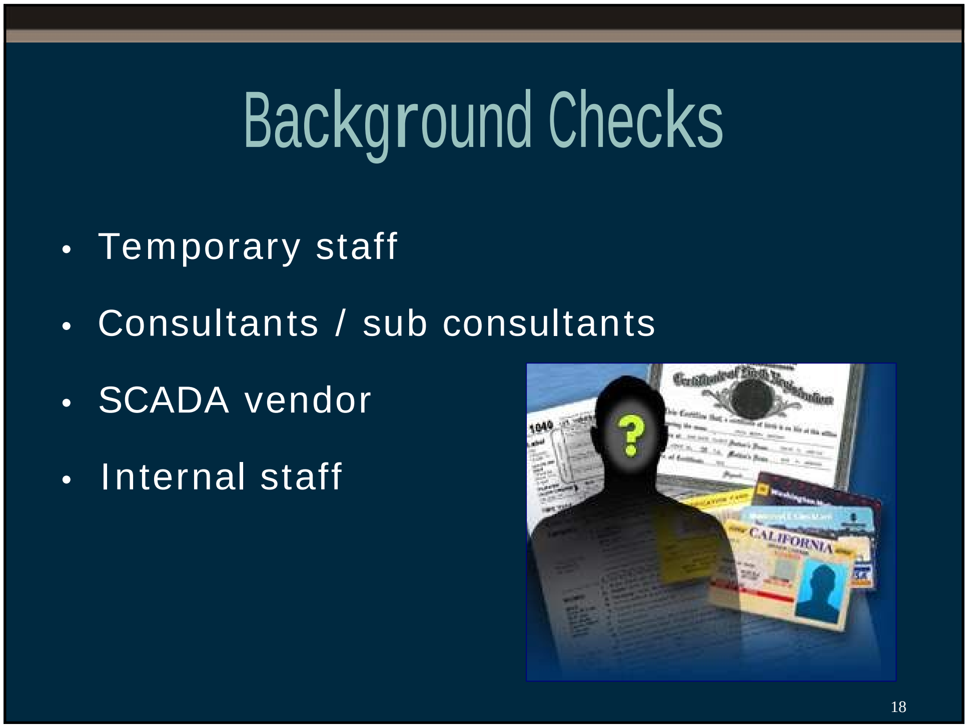
Test Complete



# Strong Physical Security

- Access to plant
- Access to control room
- Access to RTUs and PLCs
- Closed circuit cameras

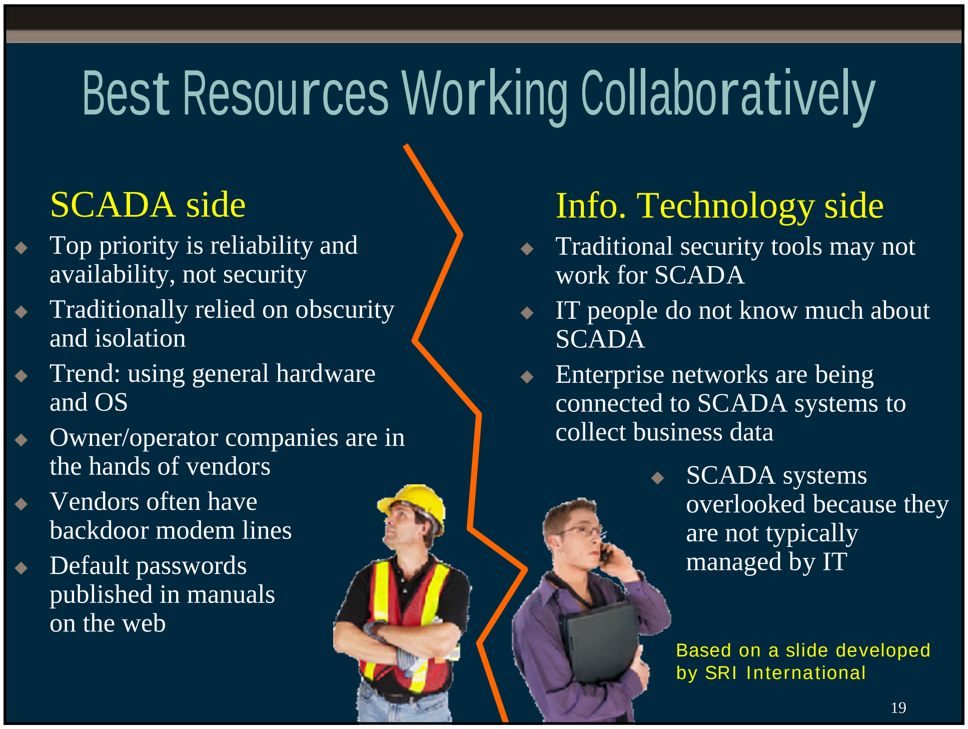
17



# Background Checks

- Temporary staff
- Consultants / sub consultants
- SCADA vendor
- Internal staff

18



## Best Resources Working Collaboratively

### SCADA side

- Top priority is reliability and availability, not security
- Traditionally relied on obscurity and isolation
- Trend: using general hardware and OS
- Owner/operator companies are in the hands of vendors
- Vendors often have backdoor modem lines
- Default passwords published in manuals on the web

### Info. Technology side

- Traditional security tools may not work for SCADA
- IT people do not know much about SCADA
- Enterprise networks are being connected to SCADA systems to collect business data
- SCADA systems overlooked because they are not typically managed by IT

Based on a slide developed by SRI International

## Water Sector Roadmap

- Plan to move forward
- 18 near-term objectives
- Regional workshops / training
- Body of knowledge

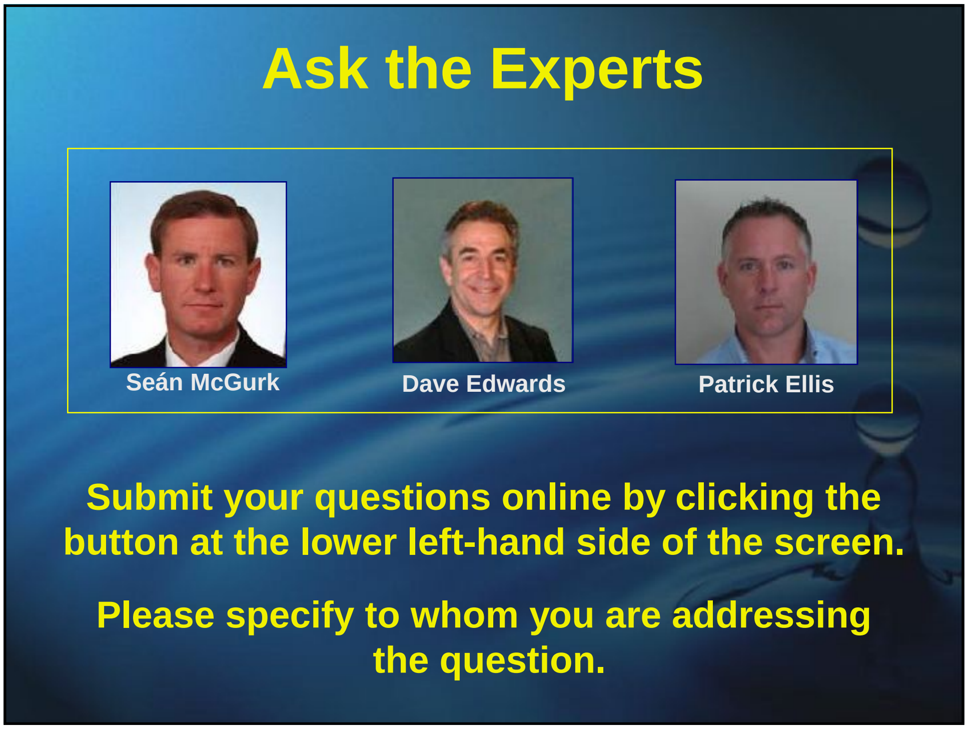
# Contacts

Seth Johnson
Water Sector Coordinating Council
Cyber Security Working Group, Chair

(408) 314-2630
sethgrp@aol.com

Dave Edwards
Process Control Systems Forum
Governing Board, Water Representative

Metropolitan Water District of So. Calif.
(213) 217-5750
dedwards@mwdh2o.com



# Ask the Experts

Seán McGurk

Dave Edwards

Patrick Ellis

Submit your questions online by clicking the button at the lower left-hand side of the screen.

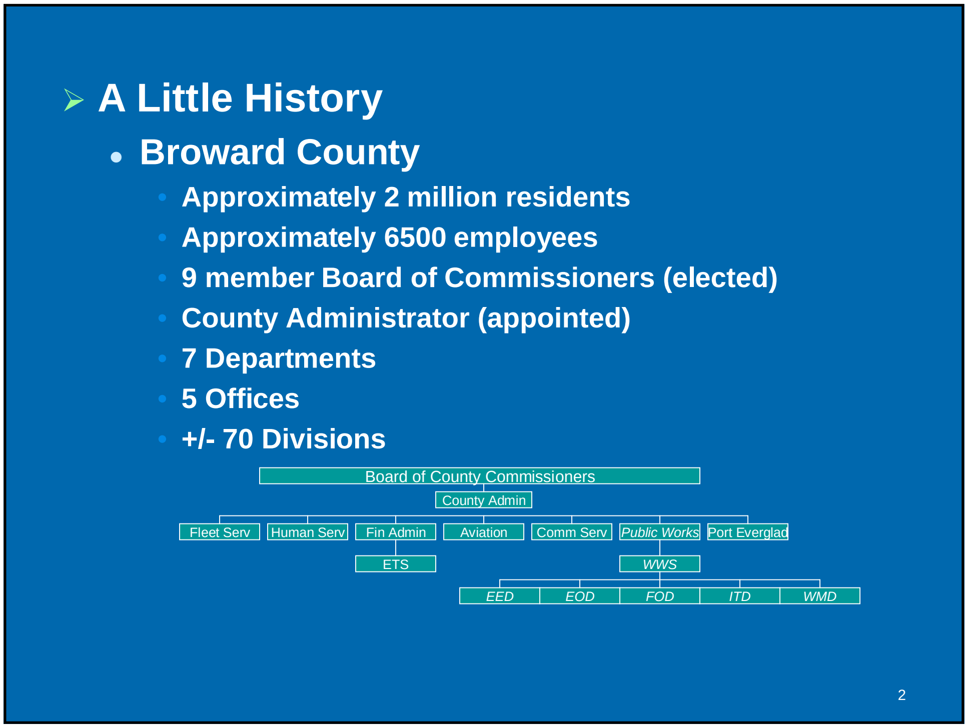
Please specify to whom you are addressing the question.

# SCADA Collaboration

## A Lessons Learned From IT

BROWARD COUNTY
FLORIDA

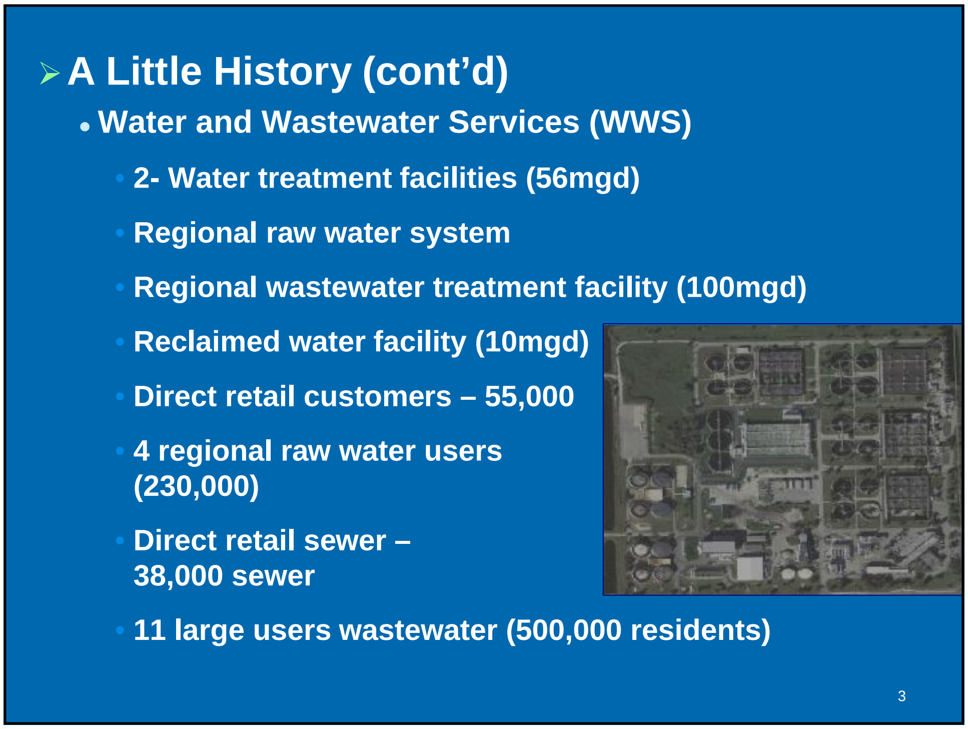
Patrick Ellis, IT Director/CISO
Broward County Water and Wastewater



## A Little History

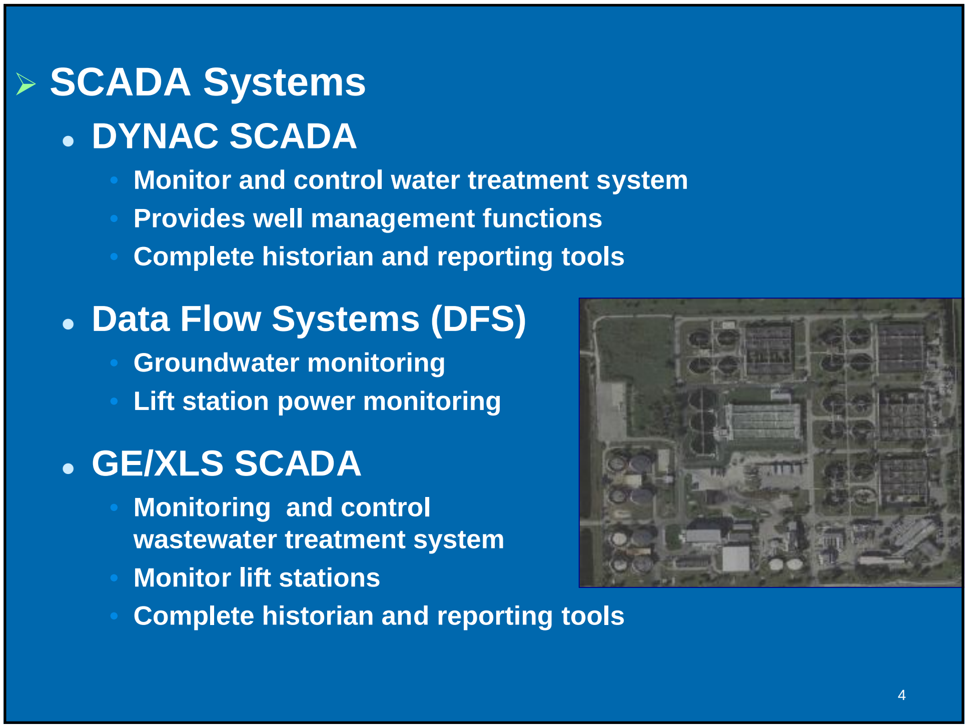
- **Broward County**
  - **Approximately 2 million residents**
  - **Approximately 6500 employees**
  - **9 member Board of Commissioners (elected)**
  - **County Administrator (appointed)**
  - **7 Departments**
  - **5 Offices**
  - **+/- 70 Divisions**

Board of County Commissioners
County Admin
Fleet Serv | Human Serv | Fin Admin | Aviation | Comm Serv | *Public Works* | Port Everglad
ETS
*WWS*
*EED* | *EOD* | *FOD* | *ITD* | *WMD*



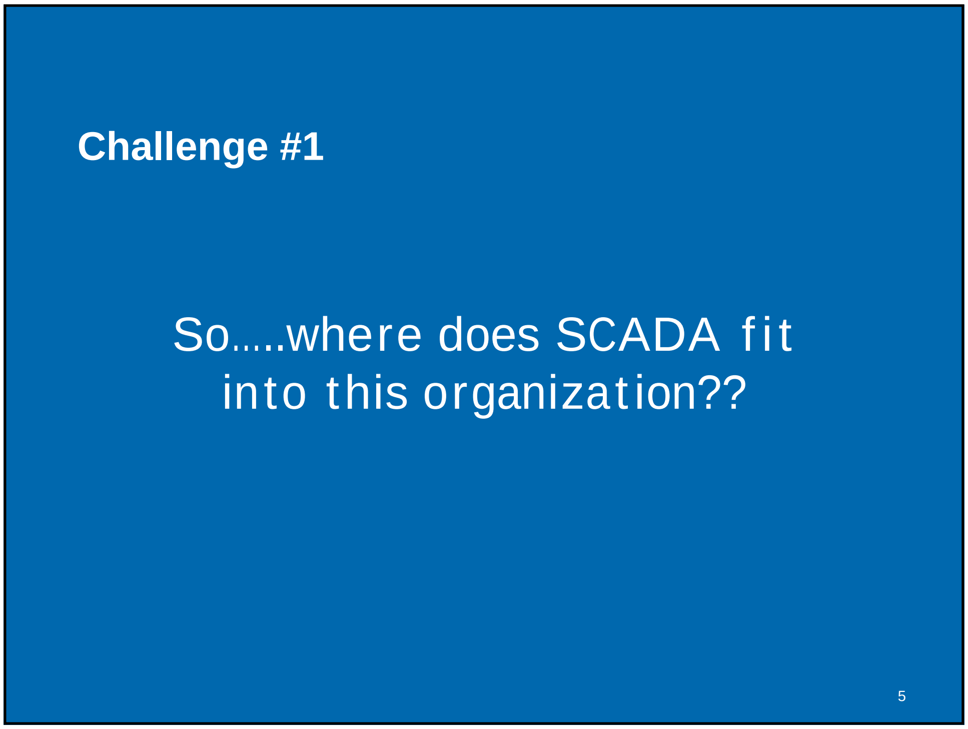
## A Little History (cont’d)

- Water and Wastewater Services (WWS)
  - 2- Water treatment facilities (56mgd)
  - Regional raw water system
  - Regional wastewater treatment facility (100mgd)
  - Reclaimed water facility (10mgd)
  - Direct retail customers – 55,000
  - 4 regional raw water users (230,000)
  - Direct retail sewer – 38,000 sewer
  - 11 large users wastewater (500,000 residents)



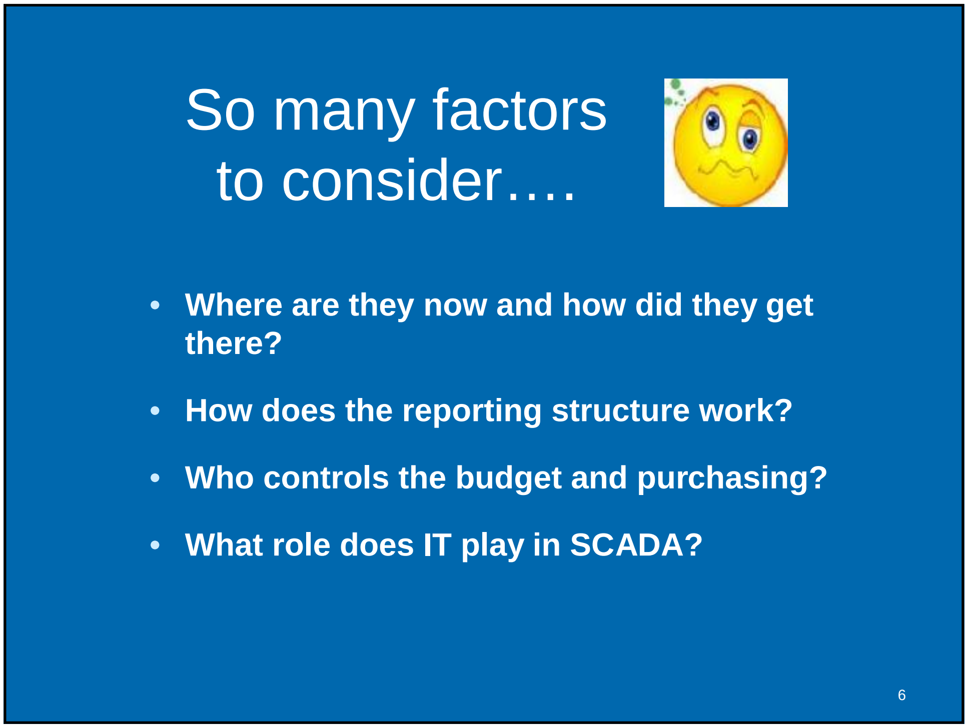
## SCADA Systems

- DYNAC SCADA
  - Monitor and control water treatment system
  - Provides well management functions
  - Complete historian and reporting tools
- Data Flow Systems (DFS)
  - Groundwater monitoring
  - Lift station power monitoring
- GE/XLS SCADA
  - Monitoring  and control wastewater treatment system
  - Monitor lift stations
  - Complete historian and reporting tools



## Challenge #1

So…..where does SCADA fit into this organization??



## So many factors to consider….

- Where are they now and how did they get there?
- How does the reporting structure work?
- Who controls the budget and purchasing?
- What role does IT play in SCADA?

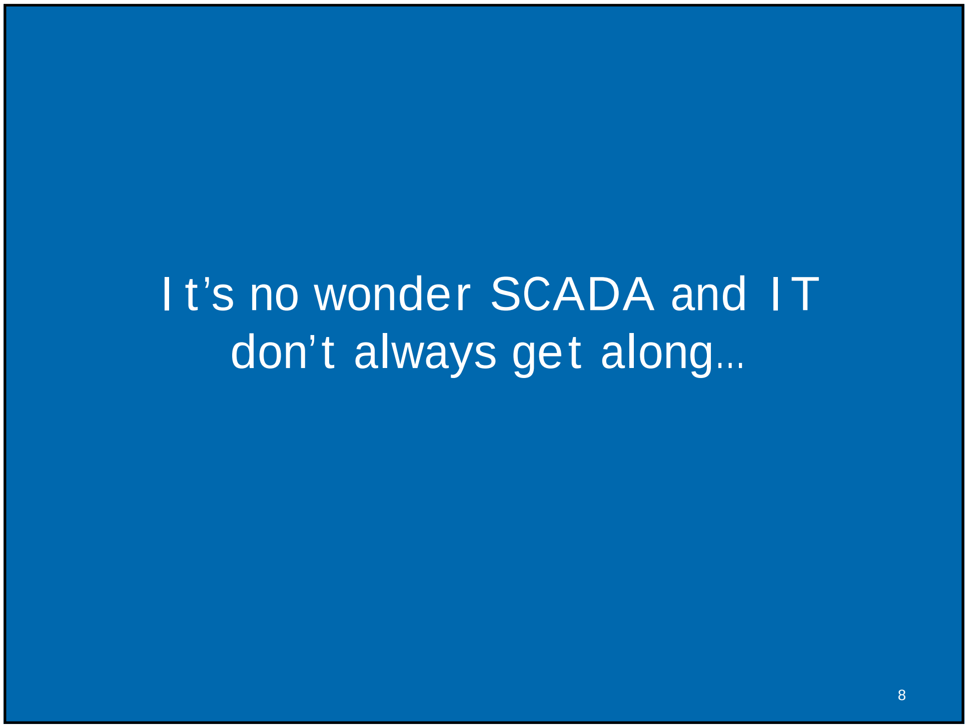
## Let’s not forget the personalities involved….

**Ladder Climbers –**
**Is there a promotion in it for me?**

**Kingdom Builders –**
**I need more people.**

**Ostrich – I don’t know,**
**I wasn’t here, I was busy.**

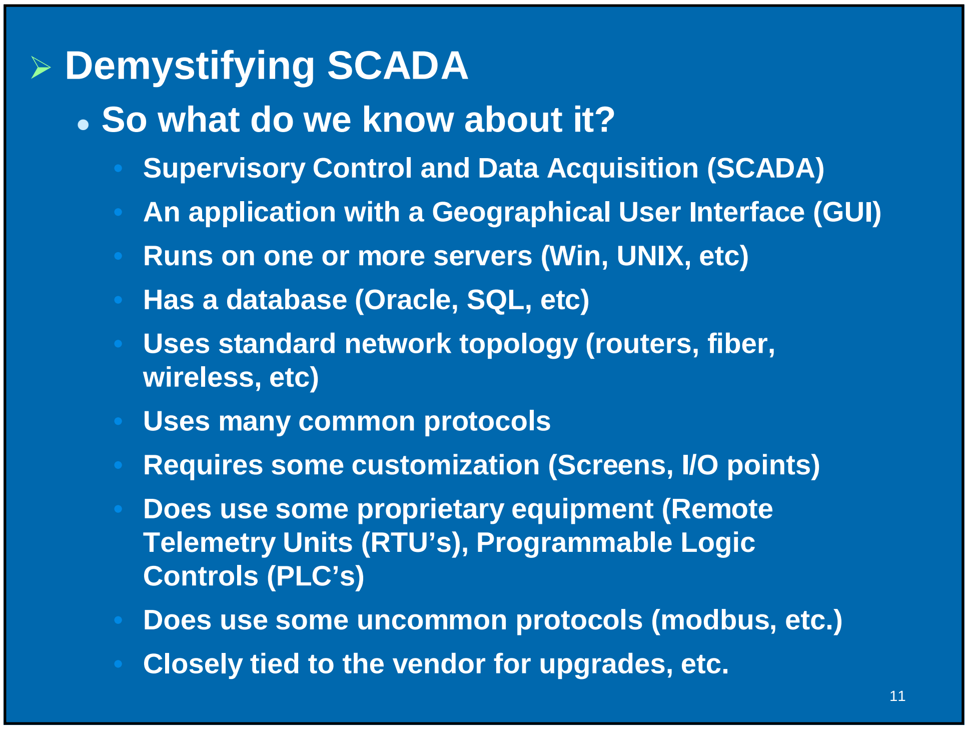
**Hermits – Just leave me alone, its your problem now.**



## It’s no wonder SCADA and IT don’t always get along…

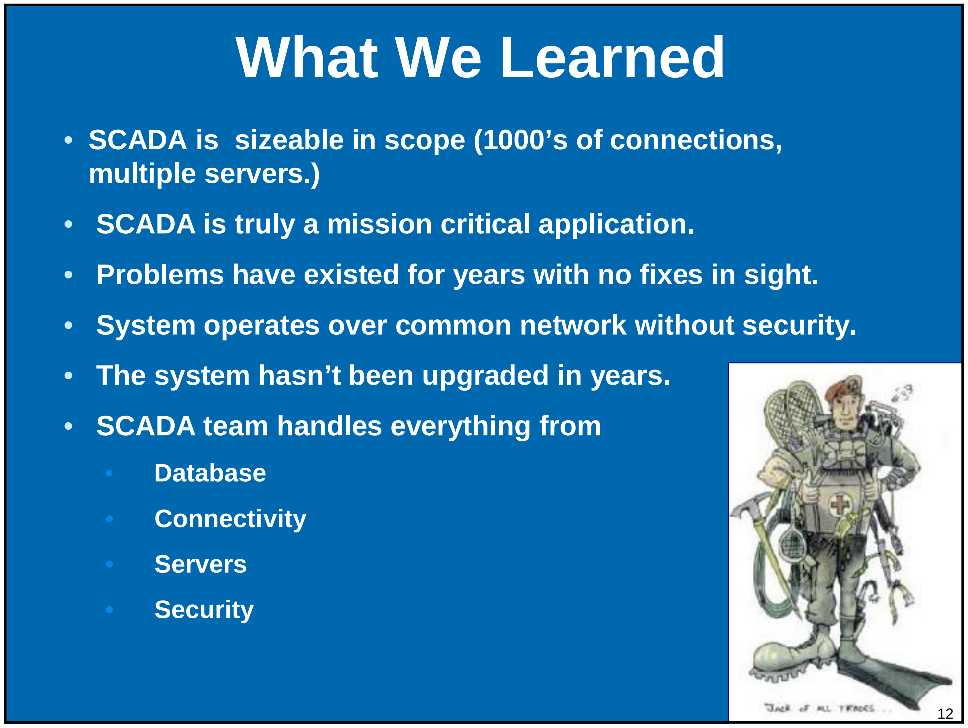
# Demystify

S.C.A.D.A.



## Demystifying SCADA

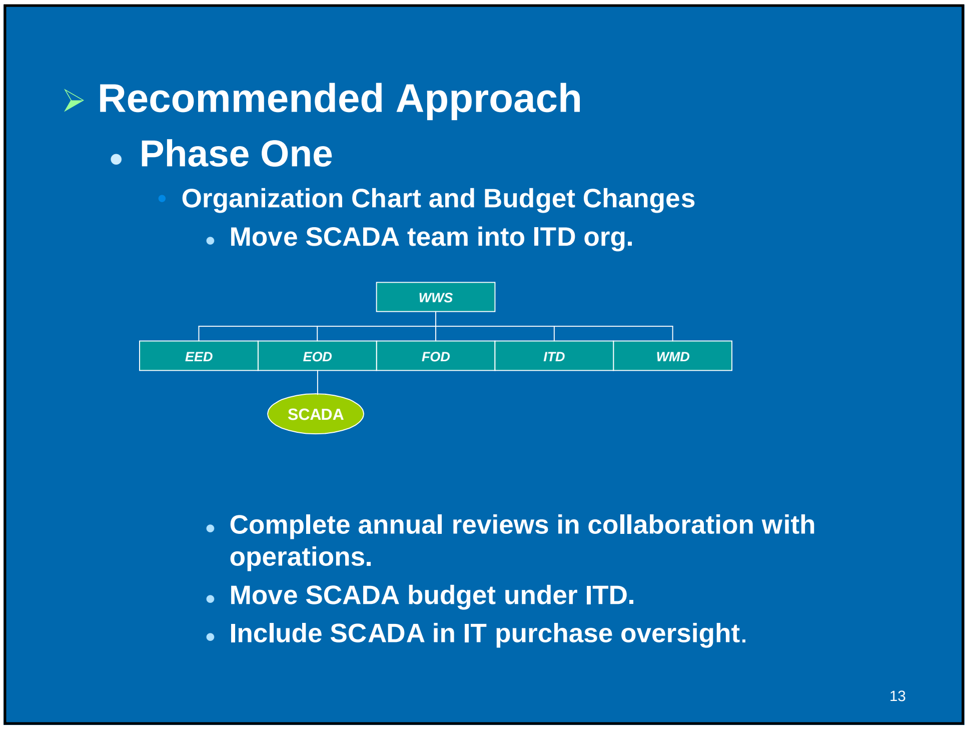
- So what do we know about it?
  - Supervisory Control and Data Acquisition (SCADA)
  - An application with a Geographical User Interface (GUI)
  - Runs on one or more servers (Win, UNIX, etc)
  - Has a database (Oracle, SQL, etc)
  - Uses standard network topology (routers, fiber, wireless, etc)
  - Uses many common protocols
  - Requires some customization (Screens, I/O points)
  - Does use some proprietary equipment (Remote Telemetry Units (RTU's), Programmable Logic Controls (PLC's)
  - Does use some uncommon protocols (modbus, etc.)
  - Closely tied to the vendor for upgrades, etc.



# What We Learned

- SCADA is  sizeable in scope (1000's of connections, multiple servers.)
- SCADA is truly a mission critical application.
- Problems have existed for years with no fixes in sight.
- System operates over common network without security.
- The system hasn't been upgraded in years.
- SCADA team handles everything from
  - Database
  - Connectivity
  - Servers
  - Security

JACK OF ALL TRADES...



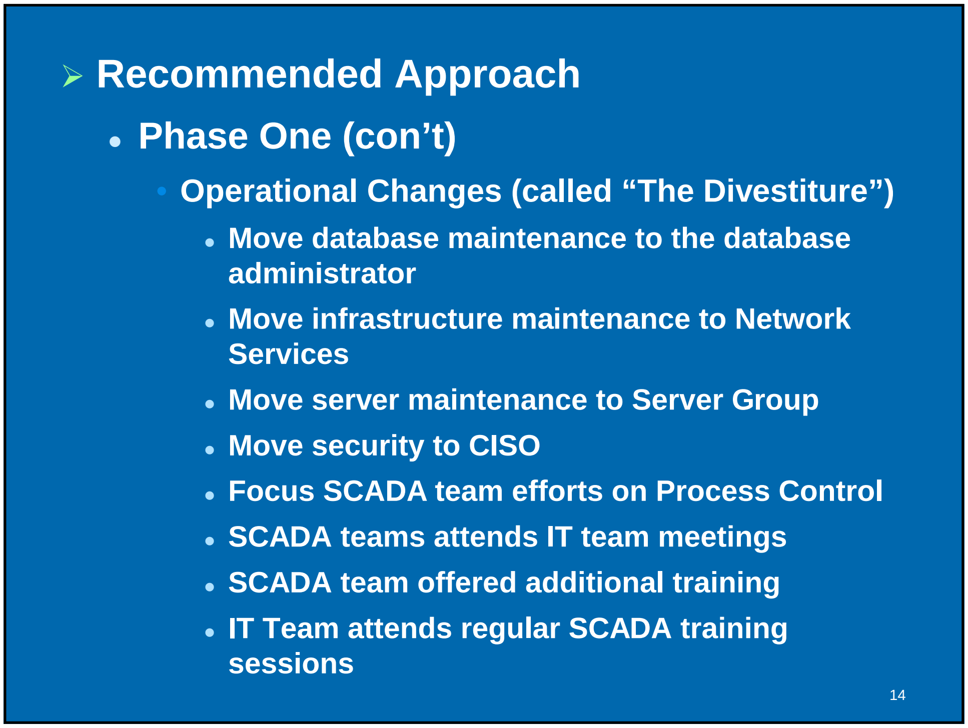
## Recommended Approach

- Phase One
  - Organization Chart and Budget Changes
    - Move SCADA team into ITD org.

WWS
EED
EOD
FOD
ITD
WMD
SCADA

- Complete annual reviews in collaboration with operations.
- Move SCADA budget under ITD.
- Include SCADA in IT purchase oversight.

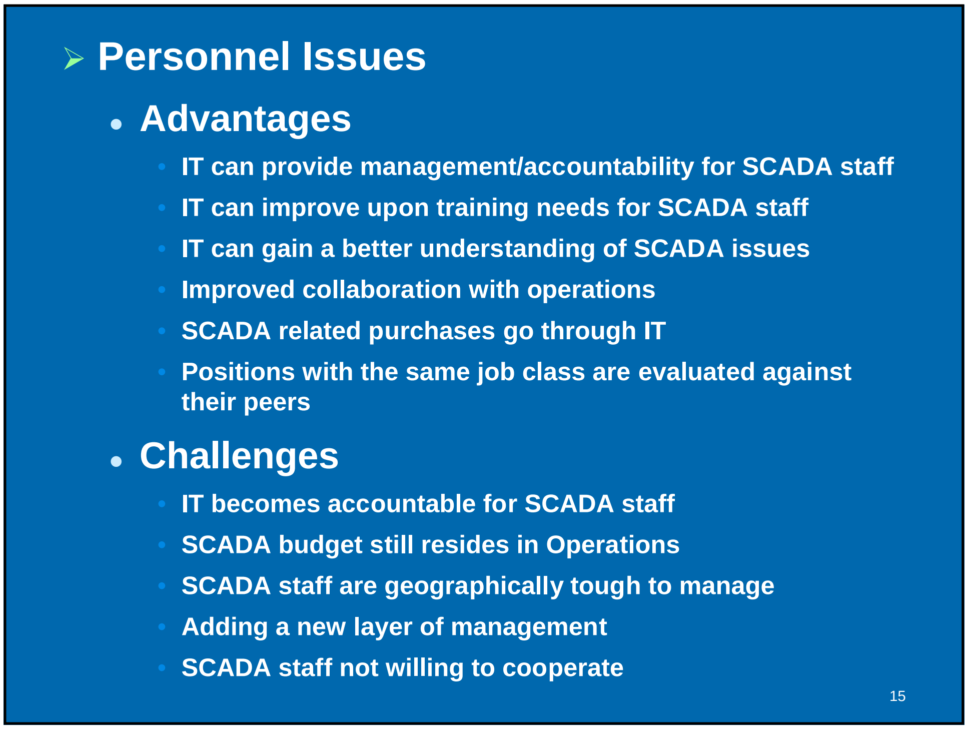
13



## Recommended Approach

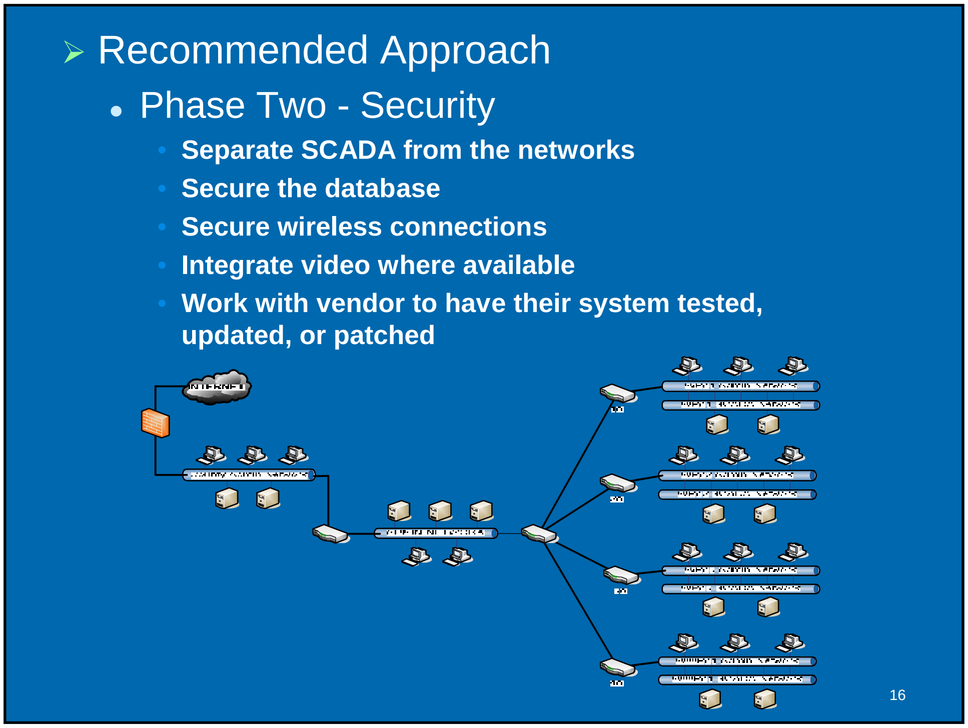
- Phase One (con’t)
  - Operational Changes (called “The Divestiture”)
    - Move database maintenance to the database administrator
    - Move infrastructure maintenance to Network Services
    - Move server maintenance to Server Group
    - Move security to CISO
    - Focus SCADA team efforts on Process Control
    - SCADA teams attends IT team meetings
    - SCADA team offered additional training
    - IT Team attends regular SCADA training sessions

14



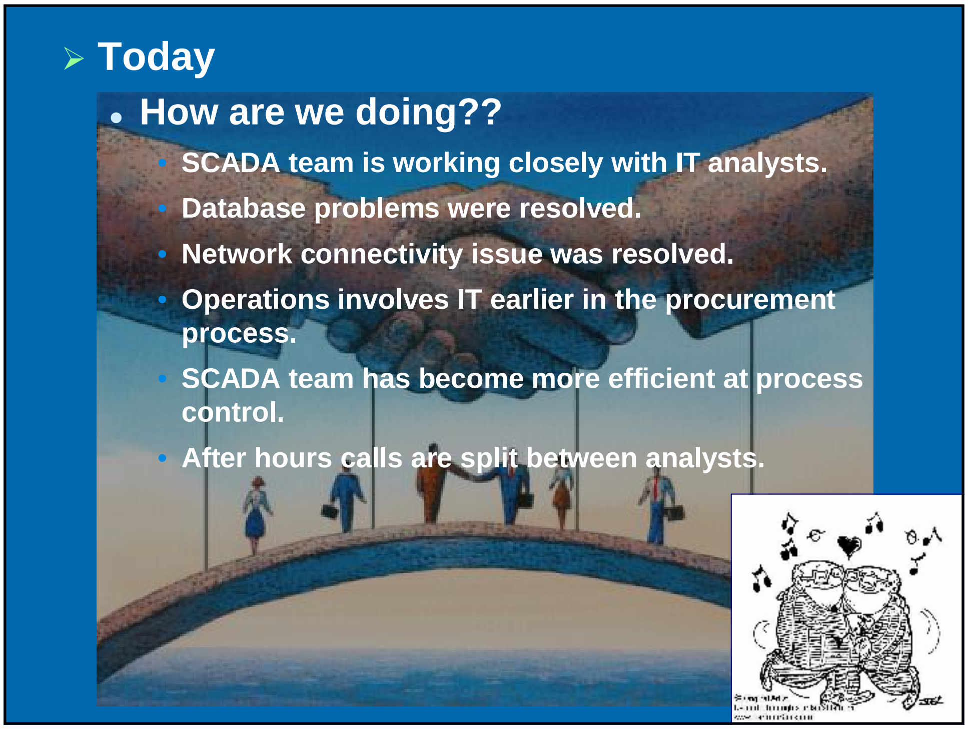
## Personnel Issues

- **Advantages**
  - IT can provide management/accountability for SCADA staff
  - IT can improve upon training needs for SCADA staff
  - IT can gain a better understanding of SCADA issues
  - Improved collaboration with operations
  - SCADA related purchases go through IT
  - Positions with the same job class are evaluated against their peers
- **Challenges**
  - IT becomes accountable for SCADA staff
  - SCADA budget still resides in Operations
  - SCADA staff are geographically tough to manage
  - Adding a new layer of management
  - SCADA staff not willing to cooperate



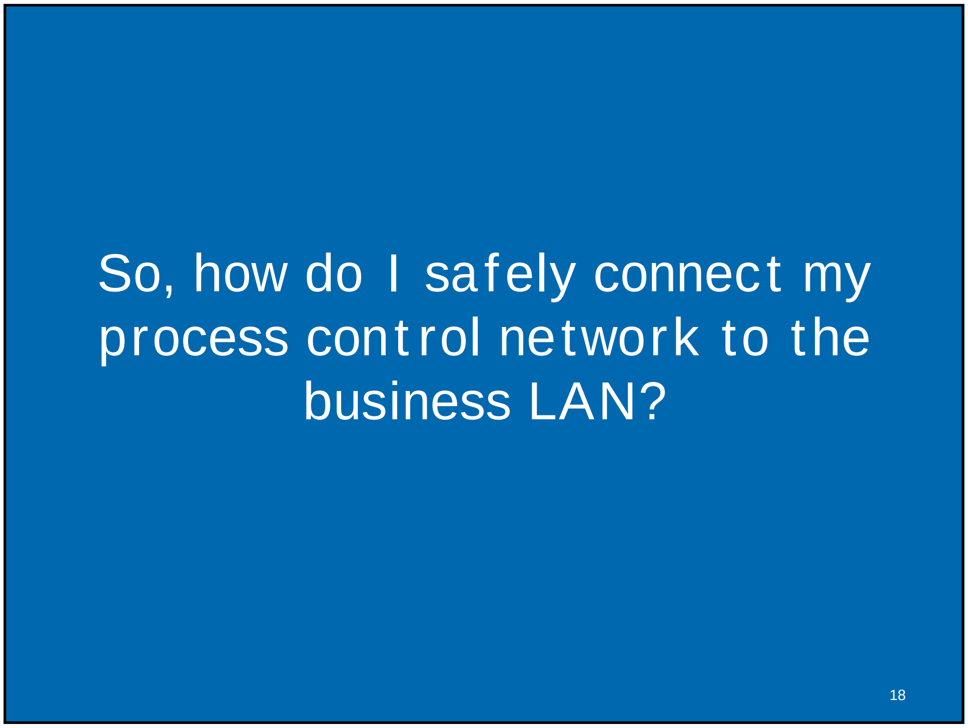
## Recommended Approach

- Phase Two - Security
  - **Separate SCADA from the networks**
  - **Secure the database**
  - **Secure wireless connections**
  - **Integrate video where available**
  - **Work with vendor to have their system tested, updated, or patched**

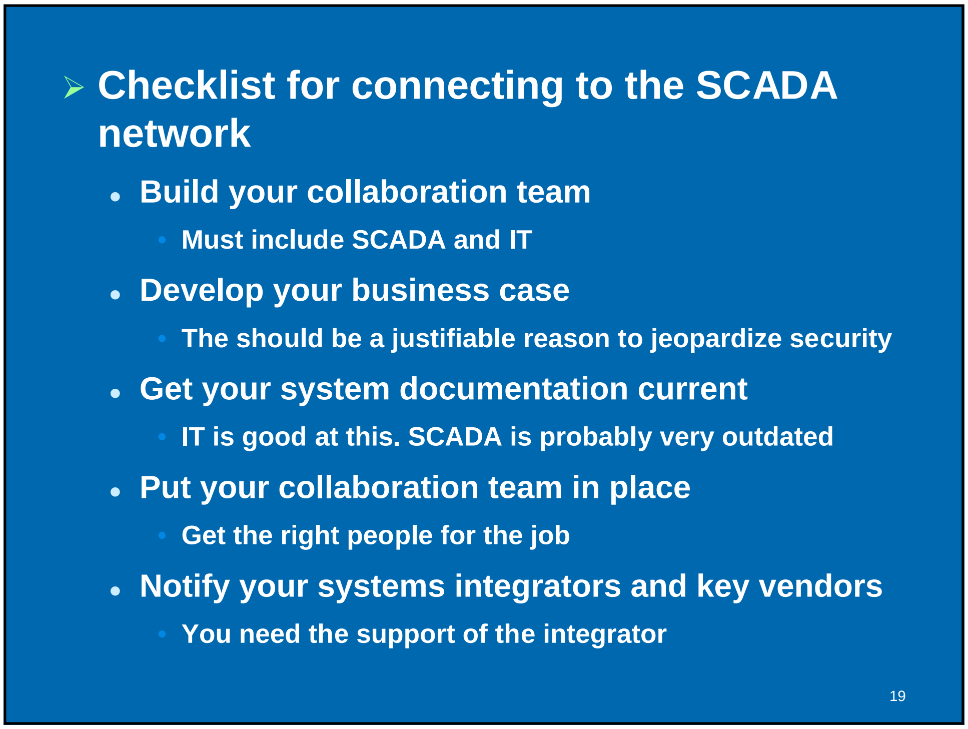


## Today

- How are we doing??
  - SCADA team is working closely with IT analysts.
  - Database problems were resolved.
  - Network connectivity issue was resolved.
  - Operations involves IT earlier in the procurement process.
  - SCADA team has become more efficient at process control.
  - After hours calls are split between analysts.

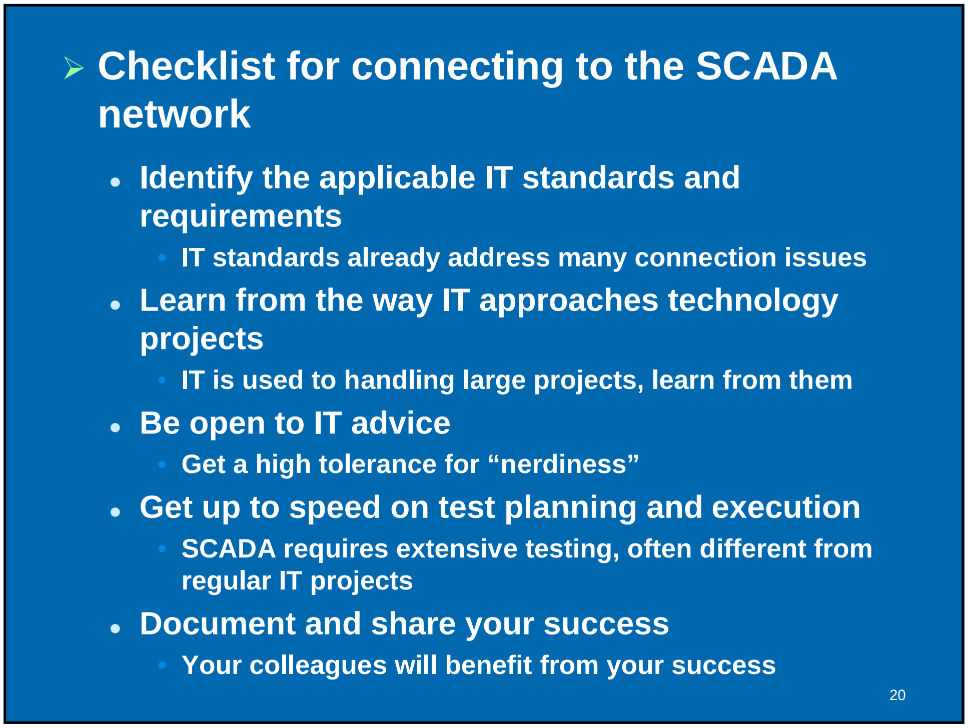


So, how do I safely connect my process control network to the business LAN?



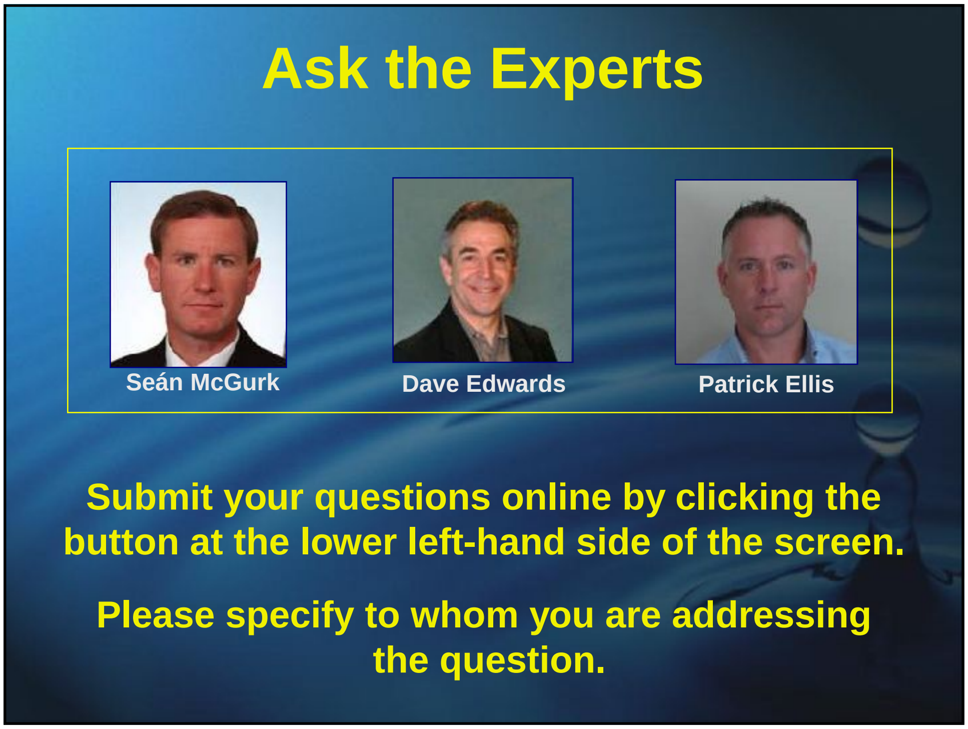
## ➢ Checklist for connecting to the SCADA network

- Build your collaboration team
  - Must include SCADA and IT
- Develop your business case
  - The should be a justifiable reason to jeopardize security
- Get your system documentation current
  - IT is good at this. SCADA is probably very outdated
- Put your collaboration team in place
  - Get the right people for the job
- Notify your systems integrators and key vendors
  - You need the support of the integrator



## ➢ Checklist for connecting to the SCADA network

- Identify the applicable IT standards and requirements
  - IT standards already address many connection issues
- Learn from the way IT approaches technology projects
  - IT is used to handling large projects, learn from them
- Be open to IT advice
  - Get a high tolerance for “nerdiness”
- Get up to speed on test planning and execution
  - SCADA requires extensive testing, often different from regular IT projects
- Document and share your success
  - Your colleagues will benefit from your success



## Ask the Experts

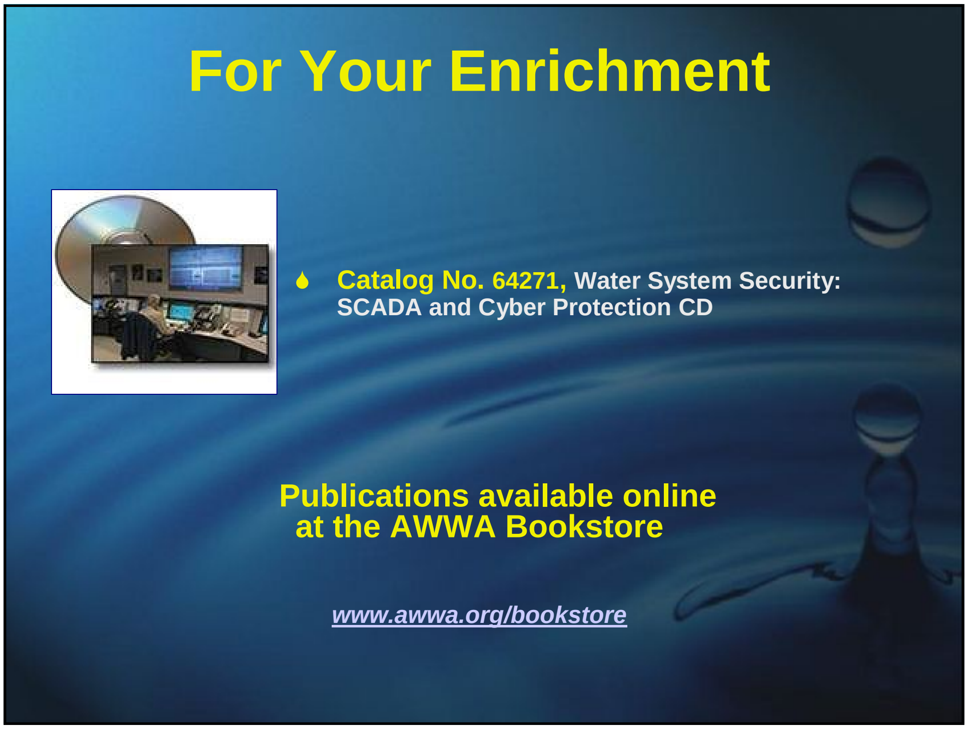
Seán McGurk

Dave Edwards

Patrick Ellis

**Submit your questions online by clicking the button at the lower left-hand side of the screen.**

**Please specify to whom you are addressing the question.**

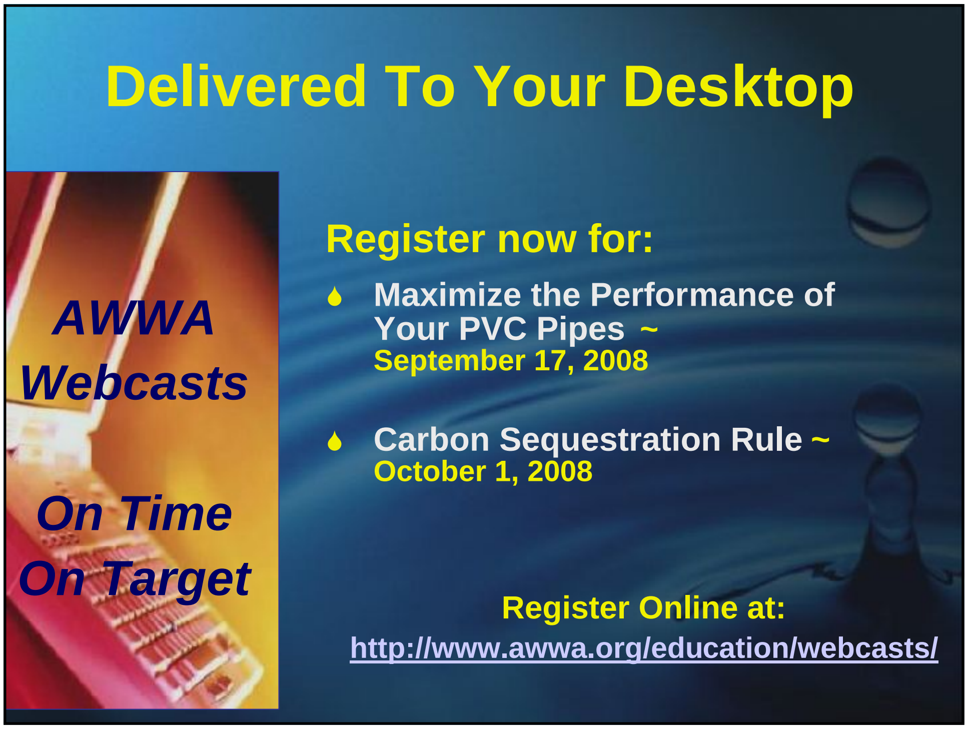


## For Your Enrichment

- **Catalog No. 64271, Water System Security: SCADA and Cyber Protection CD**

**Publications available online at the AWWA Bookstore**

*www.awwa.org/bookstore*



## Delivered To Your Desktop

AWWA Webcasts

On Time
On Target

Register now for:

- Maximize the Performance of Your PVC Pipes ~
  September 17, 2008
- Carbon Sequestration Rule ~
  October 1, 2008

Register Online at:
http://www.awwa.org/education/webcasts/

## Delivered to Your Region

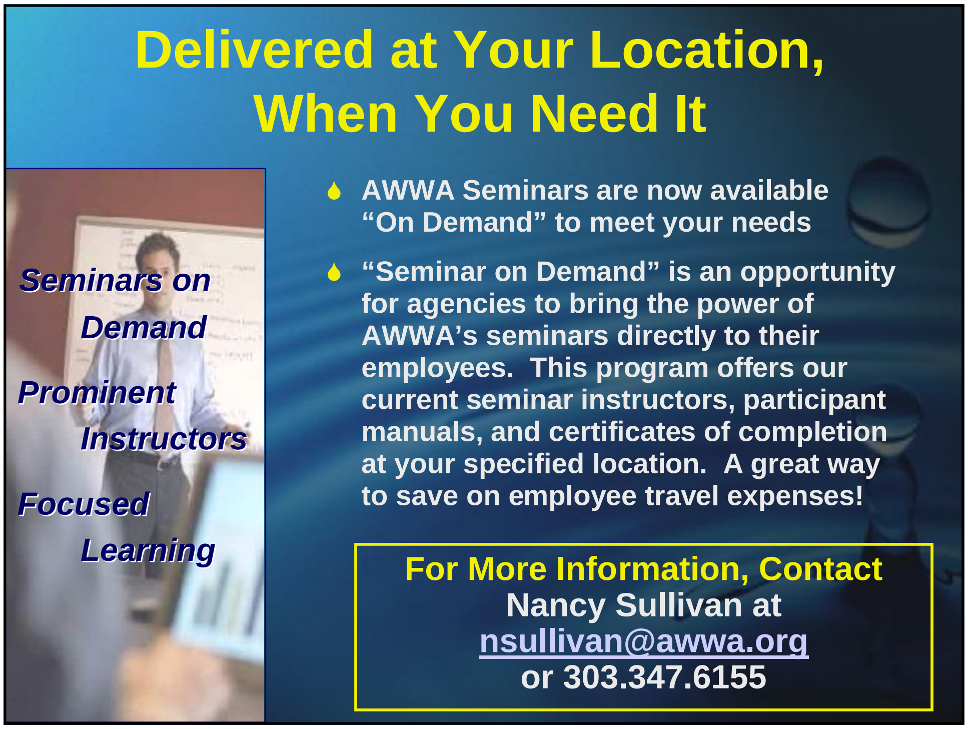
*National Seminars*

*Prominent Instructors*

*Focused Learning*

- Financial Management (3 Days)
  *Denver, CO ~*
  *October 1 - 3, 2008*

Register Online at:
www.awwa.org/education/seminars
*Conferences and Education*



# Delivered at Your Location, When You Need It

*Seminars on Demand*

*Prominent Instructors*

*Focused Learning*

- AWWA Seminars are now available "On Demand" to meet your needs
- "Seminar on Demand" is an opportunity for agencies to bring the power of AWWA's seminars directly to their employees. This program offers our current seminar instructors, participant manuals, and certificates of completion at your specified location. A great way to save on employee travel expenses!

For More Information, Contact
Nancy Sullivan at
nsullivan@awwa.org
or 303.347.6155

# Delivered for Your Specialty

- ***Distribution Systems Symposium & Exposition***
  Austin, TX - September 21 - 24, 2008

- ***Water Quality Technology Conference & Exposition (WQTC)***
  Cincinnati, OH – November 16 - 20, 2008

Register online at: www.awwa.org
*Conferences and Education*

American Water Works Association

Washington, D.C.
April 8-10
2009

# Water Security Congress

Call for Papers now open! Submit your abstract by October 1.
Visit awwa.org/conferences/security for more information.

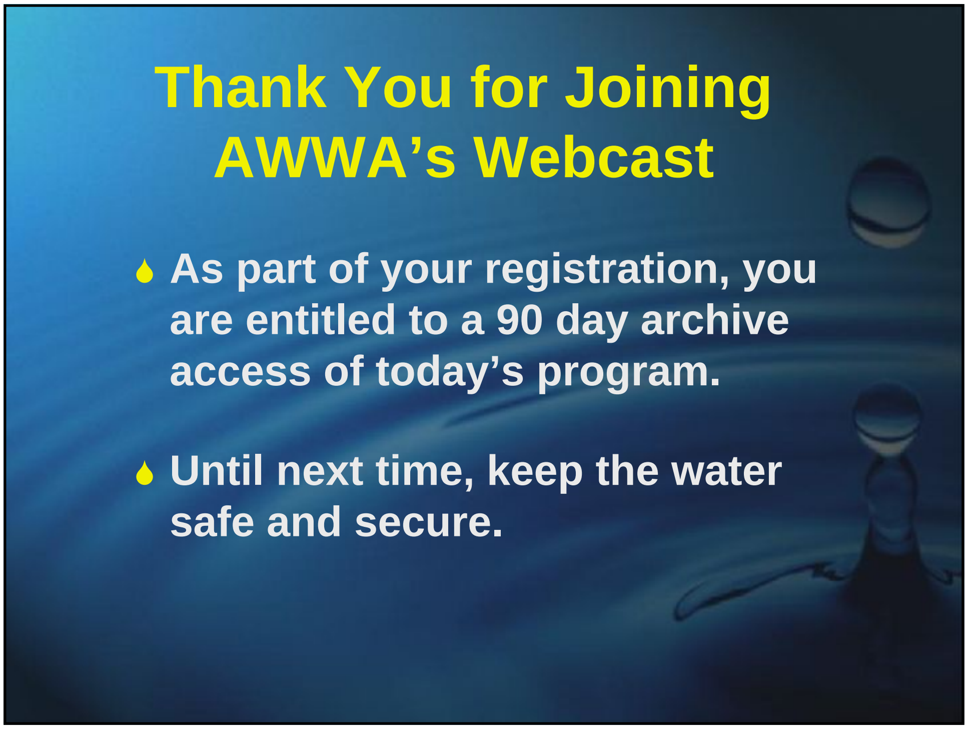
# Join Us for ACE 2009!

American Water Works Association
ACE09
ANNUAL CONFERENCE & EXPOSITION
THE World's Water EVENT

The most comprehensive and diverse water conference in the world!

June 14–18, 2009
San Diego, California

Register January 2009
www.awwa.org
Conferences and Education



## Thank You for Joining AWWA’s Webcast

- As part of your registration, you are entitled to a 90 day archive access of today’s program.
- Until next time, keep the water safe and secure.